(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 791 157**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **99 03410**

(51) Int Cl[7] : G 06 F 7/72, G 06 F 7/52, 7/50

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 17.03.99.

(30) Priorité :

(43) Date de mise à la disposition du public de la demande : 22.09.00 Bulletin 00/38.

(56) Liste des documents cités dans le rapport de recherche préliminaire : *Se reporter à la fin du présent fascicule.*

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : *STMICROELECTRONICS SA* *Société anonyme* — FR.

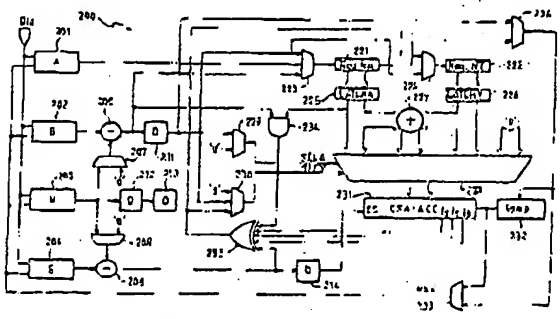
(72) Inventeur(s) : POMET ALAIN.

(73) Titulaire(s) :

(74) Mandataire(s) : CABINET BALLOT SCHMIT.

(54) DISPOSITIF ET PROCEDE DE MISE EN OEUVRE D'UNE OPERATION MODULAIRE ELEMENTAIRE SELON LA METHODE DE MONTGOMERY.

(57) La présente invention propose un coprocesseur 200 pour effectuer des opérations modulaires selon la méthode de Montgomery. Le coprocesseur de l'invention utilise un unique circuit de multiplication à accumulateur 231. La présente invention se rapporte également au procédé de calcul mis en oeuvre pour réaliser une opération modulaire avec ce coprocesseur.



FR 2 791 157 - A1

Dispositif et procédé de mise en œuvre d'une opération modulaire élémentaire selon la méthode de Montgomery.

L'invention concerne un dispositif et un procédé de mise en œuvre d'une opération modulaire élémentaire selon la méthode de Montgomery. Cette méthode permet d'effectuer des calculs modulaires dans un corps fini (ou corps de Galois) sans effectuer de divisions.

Classiquement, les opérations modulaires dans les corps finis sont utilisées en cryptographie pour des applications telles que l'authentification de messages, l'identification d'un utilisateur et l'échange de clés. De tels exemples d'applications sont décrits par exemple dans la demande de brevet FR-A-2 679 054 (ci-après D1).

On trouve dans le commerce des circuits intégrés dédiés à de telles applications, par exemple le produit fabriqué par STMicroelectronics S.A. et référencé ST16CF54, bâti autour d'une association de type unité centrale - coprocesseur arithmétique, et dédié à la mise en œuvre de calculs modulaires. Le coprocesseur utilisé permet de traiter des multiplications modulaires, en utilisant la méthode de Montgomery. Il fait l'objet de la demande de brevet EP-A-0 601 907 (ci-après D2).

L'opération de base, dite P_{field}, consiste, à partir de trois données binaires, A (multiplicande), B (multiplieur inférieur à N) et N (modulo), codées sur un nombre entier n de bits, à produire une donnée binaire notée $P(A, B)_N$ codée sur n bits, telle que $P(A, B)_N = A * B * I \bmod N$, avec $I = 2^{-n} \bmod N$. Pour cela, on considère que les données sont codées sur m mots de k bits, avec $m * k = n$, et on fournit les mots A et B à un circuit de multiplication ayant une entrée série, une entrée parallèle et une sortie série.

Pour le coprocesseur décrit dans D2, on a $k = 32$ et $m = 8$ ou 16. La figure 1 représente le coprocesseur d'arithmétique modulaire dévoilé par D2. Ce coprocesseur

comprend les éléments suivants:

- trois registres à décalage 10, 11, et 12, de m * k bits, destinés à recevoir respectivement le multiplieur B, le résultat S, et le modulo N,
- des multiplexeurs 13 à 15 dont les sorties sont reliées respectivement aux entrées des registres 10 à 12,
- trois registres à décalage 16, 17, et 18, de k bits, ayant une entrée série et une sortie parallèle, destinés à recevoir respectivement k bits du multiplicande A, un paramètre de calcul noté J_0, un résultat intermédiaire noté Y_0,
- deux circuits de multiplication 19 et 20 ayant chacun une entrée série, une entrée parallèle de k bits et une sortie série,
- deux bascules parallèles 21 et 22 de k bits qui servent de tampon aux circuits de multiplication 19 et 20,
- un multiplexeur 23 qui sert à relier le registre 22 soit au registre 17, soit au registre 18,
- trois multiplexeurs 24, 25 et 26 servant à aiguiller les données sur les entrées des circuits de multiplication 19 et 20,
- trois circuits de soustraction 27, 28, et 29 comportant chacun deux entrées séries et une sortie série,
- deux circuits d'addition 30 et 31, ayant chacun deux entrées séries et une sortie série,
- trois cellules à retard 32, 33 et 34 qui sont en fait des registres à décalage de k bits, et qui servent à retarder les données de k cycles d'horloge pour masquer le temps de calcul des circuits de multiplication 19 et 20,
- un circuit de comparaison 35,
- deux multiplexeurs 36 et 37 qui permettent le contrôle des circuits de soustraction 27 et 28,
- un multiplexeur 38, et

- un démultiplexeur 39.

Pour plus de détails sur la réalisation de ces éléments on peut se référer à D2.

Pour réaliser une opération élémentaire dite P_{Field} du type $P_{Field}(A, B)_N = A * B * I \bmod N$, A et B étant codés sur m mots de k bits, et I étant une erreur égale à 2^{-m*k}, on réalise m fois l'itération de boucle suivante avec i un indice variant de 0 à m-1 :

$X = S(i-1) + A_i * B$,

$Y_0 = (X * J_0) \bmod 2^k$,

$Z = X + (N * Y_0)$

$S(i) = Z \setminus 2^k$, \ étant une division entière,

si S(i) est supérieur à N alors on soustrait N à S(i) avant la prochaine itération,

avec $S(-1) = 0$, A_i étant le mot de k bits de poids i, J_0 étant un mot de k bits défini par l'équation $((N * J_0) + 1) \bmod 2^k = 0$.

Le coprocesseur de la figure 1 permet d'effectuer une itération complète par un décalage simultané de m * k bits des registres 10 à 12 contenant respectivement B, S(i-1) et N suivi d'un décalage de 2 * k bits du registre 12 pour mémoriser S(i), le mot A_i étant chargé dans le registre 21, et le mot J_0 étant chargé dans le registre 17. Pour réaliser le calcul complet de $P_{Field}(A, B)_N$, il suffit de répéter m fois chaque itération en changeant le mot A_i contenu dans le registre 21 lors de chaque itération.

L'opération « $X = S(i-1) + A_i * B$ » se fait à l'aide des circuits de multiplication 19 et d'addition 30. L'opération « $Y_0 = (X * J_0) \bmod 2^k$ » se fait, lors des k premiers décalages, dans le circuit de multiplication 20, en ayant pris soin de mémoriser J_0 dans le registre 22, le résultat Y_0 étant mémorisé dans le registre 18. L'opération « $Z = X + (N * Y_0)$ », N et X ayant été retardés de k bits dans les cellules à retard 32 et 34 et Y_0 ayant été mis dans le registre 22,

s'effectue à l'aide des circuits de multiplication 20 et d'addition 31. L'opération « $S(i) = Z \setminus 2^k$ » est réalisée par décalage de k bits. La comparaison de S(i) avec N s'effectue par la soustraction de N à S(i) dans le circuit de soustraction 29, N étant retardé de k bits dans la cellule 33, un éventuel débordement étant détecté et mémorisé dans le circuit de comparaison 35 pour connaître le résultat de la comparaison. La soustraction de N à S(i) se faisant lors de l'itération suivante dans le circuit de soustraction 28.

De nombreuses améliorations ont été réalisées sur ce circuit. Les améliorations ayant pour but d'aller plus vite et/ou de réduire la taille du circuit et/ou de réduire la consommation du circuit et/ou d'apporter des fonctionnalités supplémentaires sans augmenter la taille du circuit de manière considérable. L'homme du métier peut se reporter entre autre aux publications des demandes de brevets européens EP - 0 712 070, EP - 0 712 071, EP - 0 712 072, EP - 0 778 518, EP - 0 784 262, EP - 0 785 502, EP - 0 785 503, EP - 0 793 165, EP - 0 853 275, et également à la publication de la demande de brevet internationale WO/97 25668.

Il est également connu, de la publication de la demande de brevet européen EP - 0 566 498 (ci-après D3), un autre circuit permettant de calculer l'opération élémentaire $P(A, B)_N = A * B * I \bmod N$, avec $I = 2^{-n}$ et n la taille de A, B ou N. Le circuit de D3 utilise un unique circuit de multiplication parallèle/série, représenté dans D3 sous la forme d'un additionneur parallèle couplé à un registre à décalage. Le circuit de D3 ne reproduit pas exactement l'algorithme de Montgomery et utilise une donnée intermédiaire égale à (N-1)/2+1. Le circuit de D3 utilise un circuit de multiplication disposant d'une entrée parallèle de n bits et se limite à des opérandes de calcul de taille figée. Par ailleurs, la taille du circuit de D3 est proportionnelle à la taille

des opérandes utilisés, la surface ainsi occupée étant considérable.

La présente invention a pour but d'améliorer l'état de la technique en proposant un coprocesseur dont les performances en vitesse de traitement sont améliorées par rapport au circuit de D2, tout en occupant une surface plus réduite de silicium. Le coprocesseur de l'invention utilise un unique circuit de multiplication d'architecture voisine de D3. La présente invention se rapporte également au procédé de calcul mis en œuvre pour réaliser une opération modulaire.

L'invention a pour objet un circuit intégré comprenant un coprocesseur d'arithmétique modulaire comportant des moyens de mémorisation pour mémoriser et fournir en série des premier et deuxième opérandes A et B, un modulo N et un résultat S, avec A un entier codé sur a * k bits, a étant un entier non nul au plus égal à m, et avec B, N et S qui sont des entiers codés sur au plus m * k bits, m et k étant des entiers supérieurs à 1, et des moyens de calcul pour effectuer des opérations modulaires selon la méthode de Montgomery, caractérisé en ce que les moyens de calcul comportent un circuit pour calculer une donnée intermédiaire Y_0; une première bascule de k bits pour mémoriser un mot A_i de k bits de A; une deuxième bascule de k bits pour mémoriser soit le mot de poids le plus faible de N soit Y_0; un circuit parallèle d'addition connecté pour additionner les mots contenus dans les première et deuxième bascules; un dispositif de sélection couplé aux sorties des première et deuxième bascules et du circuit parallèle d'addition afin de fournir sur une sortie parallèle soit le mot contenu dans la première bascule, soit le mot contenu dans la deuxième bascule, soit la somme des mots contenus dans les première et deuxième bascules, soit "zéro", en fonction d'une part d'un bit de B, et d'autre part soit d'un bit de Y_0 soit d'un bit de N; un circuit accumulateur qui

additionne, décale d'un bit et mémorise les mots fournis successivement par le dispositif de sélection avec un bit d'un résultat actualisé S, le bit sortant du circuit accumulateur devenant un nouveau résultat actualisé.

Une amélioration de l'invention consiste en ce que les moyens de calcul comportent un premier registre à décalage de k bits pour recevoir d'une part un mot de k bits de A et transmettre ledit mot en parallèle à la première bascule et d'autre part N afin de retarder N de k cycles d'un signal d'horloge.

L'invention concerne également un procédé pour effectuer une opération modulaire selon la méthode de Montgomery par décalage en série de premier et deuxième opérandes A et B, d'un modulo N et d'un résultat actualisé à travers des moyens de calcul, avec A un entier codé sur a * k bits, a étant un entier non nul au plus égal à m, et avec B, N et S des entiers codés sur au plus m * k bits, m et k étant des entiers supérieurs à 1 caractérisé en ce qu'il comporte la répétition des étapes suivantes, i étant un indice variant de 0 à m-1: mémorisation d'un mot A_i de k bits correspondant au mot de poids i de A dans une première bascule de k bits; calcul d'une donnée intermédiaire Y_0 telle que $Y_0 = ((S(i-1) + (Ai * B)) * J_0) \bmod 2^k$, avec S(i-1) qui correspond au (i-1)-ième résultat actualisé, S(-1) étant égal à 0, et J_0 étant un mot de k bits résolvant l'équation $((J_0 * N) + 1) \bmod 2^k = 0$; mémorisation du mot de k bits de poids faible de N puis de Y_0 dans une deuxième bascule de k bits; addition dans un circuit parallèle d'addition des mots contenus dans les première et deuxième bascules; sélection et fourniture soit du mot contenu dans la première bascule, soit du mot contenu dans la deuxième bascule, soit de la somme des mots contenus dans les première et deuxième bascules, soit "zéro", en fonction d'une part d'un bit de B, et d'autre part soit d'un bit de Y_0 soit d'un bit de N; Additions successives dans un

circuit accumulateur des mots fournis par le dispositif de sélection pour chaque paire de bits de B et de N, le résultat de chaque addition étant additionné à un bit du précédent résultat actualisé S(i-1) puis décalé d'un bit et mémorisé entre chaque addition, le bit sortant de l'accumulateur lors du décalage correspondant à un nouveau résultat actualisé S(i).

Une amélioration consiste en ce que l'on effectue une comparaison du résultat sortant de l'accumulateur avec N retardé de k cycles d'un signal d'horloge, et en ce que l'on utilise un même premier registre à décalage de k bits pour retarder N et pour pouvoir charger les mots A_i dans la première bascule. De plus, la mémorisation d'un mot A_i dans la première bascule s'effectue par k décalages du mot A_i dans le premier registre puis chargement parallèle dans la première bascule après que le mot A_i ait été chargé en entier dans le premier registre. Le calcul de chaque bit de la donnée intermédiaire Y_0 s'effectue un cycle d'horloge avant que l'on ait besoin dudit chaque bit.

L'invention sera mieux comprise et d'autres particularités et avantages apparaîtront à la lecture de la description qui va suivre, la description faisant référence aux dessins annexés parmi lesquels :

la figure 1 représente un coprocesseur d'arithmétique modulaire selon l'état de la technique,

la figure 2 représente un coprocesseur d'arithmétique modulaire selon l'invention, et

les figures 3 à 7 représentent de manière détaillée différents éléments du coprocesseur de la figure 2.

La figure 1 ayant été décrite précédemment et représentant l'état de la technique, elle ne sera pas décrite plus en détail.

La figure 2 représente le coprocesseur 200 d'arithmétique modulaire, selon un mode préféré de réalisation. Afin de ne pas surcharger le schéma, seul le

cheminement des données a été représenté sur cette figure 2. Une machine d'état (non représentée) envoie les signaux de commande nécessaires aux différents éléments fonctionnels du coprocesseur 200. Le coprocesseur 200 comporte les éléments suivants:

- Des premier à quatrième dispositifs de mémorisation 201 à 204 contenant respectivement des données A, B, N et S. Les données A, B, N et S sont des données codées sur au plus m mots de k bits. Les dispositifs de mémorisation 201 à 204 permettent de fournir de manière indépendante n'importe quel mot de k bits de la donnée mémorisée. Chaque dispositif de mémorisation 201 à 204 dispose de première et deuxième entrées séries et d'une sortie de donnée de type série. La première entrée de chaque dispositif de mémorisation 201 à 204 est connectée à une borne d'entrée Din.

- Des premier et deuxième circuits de soustraction 205 et 206 de type série disposent de première et deuxième entrées et d'une sortie de type série. La première entrée du premier circuit de soustraction 205 est connectée à la sortie du deuxième dispositif de mémorisation 202. La première entrée du deuxième circuit de soustraction 206 est connectée à la sortie du quatrième dispositif de mémorisation 204.

- Des premier et deuxième multiplexeurs 207 et 208 sont couplés respectivement aux deuxièmes entrées des premier et deuxième circuits de soustraction 205 et 206. Les premier et deuxième multiplexeurs 207 et 208 disposent de deux entrées chacun, l'une des entrées recevant un "zéro" logique, et l'autre des entrées étant connectée à la sortie du troisième dispositif de mémorisation 203. L'association des premier et deuxième circuits de soustraction 205 et 206 avec les premier et deuxième multiplexeurs 207 et 208 permet de soustraire soit "zéro" soit la donnée sortante du troisième dispositif de mémorisation 203 aux données sortantes des

deuxième et quatrième dispositifs de mémorisation 202 et 204.

- Des premier à quatrième circuits de retard 211 à 214 servent à synchroniser les données en les retardant d'un cycle du signal d'une horloge de cadencement. Chacun des circuits de retard 211 à 214 dispose d'une entrée et d'une sortie, chaque circuit de retard étant par exemple constitué d'une simple bascule synchrone de type D. L'entrée du premier circuit de retard 211 est connectée à la sortie du premier circuit de soustraction 205. L'entrée du deuxième circuit de retard 212 est connectée à la sortie du troisième dispositif de mémorisation 203. L'entrée du troisième circuit de retard 213 est connectée à la sortie du deuxième circuit de retard 212. L'entrée du quatrième circuit de retard 214 est connectée à la sortie du deuxième circuit de soustraction 206.

- Un premier registre 221 à décalage de k bits dispose d'une entrée série, d'une sortie série et d'une sortie parallèle. Ce premier registre 221 sert d'une part de registre tampon pour les mots de A et d'autre part de retardateur de k cycles d'horloge pour N.

- Un deuxième registre 222 à décalage de k bits dispose d'une entrée série et d'une sortie parallèle. Ce deuxième registre 222 sert d'une part de registre tampon pour le mot N_0 de poids le plus faible de N et d'autre part pour une donnée intermédiaire Y_0.

- Un troisième multiplexeur 223 est associé au premier registre 221. Le troisième multiplexeur 223 dispose de trois entrées et d'une sortie, la sortie étant connectée à l'entrée du premier registre 221. L'une des entrées du troisième multiplexeur 223 est connectée à la sortie du premier dispositif de mémorisation 201. Une autre des entrées du troisième multiplexeur est connectée à la sortie du premier circuit de soustraction 205. La dernière des entrées du troisième multiplexeur 223 est connectée à la sortie du troisième circuit de retard 213.

- Un quatrième multiplexeur 224 est associé au deuxième registre 222. Le quatrième multiplexeur 224 dispose de première et deuxième entrées et d'une sortie, la sortie étant connectée à l'entrée du deuxième registre 222. La première entrée du quatrième multiplexeur 224 est connectée à la sortie du troisième circuit de retard 213.

- Des première et deuxième bascules 225 et 226 à verrouillage de k bits servent à mémoriser pendant le calcul d'une part un mot de A et d'autre part le mot N_0 de poids le plus faible de N ou la donnée intermédiaire Y_0. Chacune des bascules 225 et 226 comporte une entrée parallèle et une sortie parallèle, les entrées des première et deuxième bascules 225 et 226 étant respectivement connectées aux sorties parallèles des premier et deuxième registres 221 et 222.

- Un circuit d'addition 227, disposant de deux entrées parallèles et d'une sortie parallèle, a ses deux entrées connectées respectivement aux sorties des première et deuxième bascules 225 et 226. La sortie du circuit d'addition 227 fournit ainsi la somme des contenus des première et deuxième bascules 225 et 226.

- Un dispositif de sélection 228 est connecté aux sorties des première et deuxième bascules 225 et 226 et à la sortie du circuit d'addition 227 afin de pouvoir fournir sur une sortie parallèle soit le contenu de la première bascule 225, soit le contenu de la deuxième bascule 226, soit la somme des contenus des première et deuxième bascules 225 et 226, soit "zéro". Le dispositif de sélection 228 dispose en outre de première et deuxième entrées de sélection qui reçoivent respectivement un premier signal de sélection SELA et un deuxième signal de sélection SELY. Lorsque les premier et deuxième signaux SELA et SELY de sélection sont tous deux à un niveau logique "zéro", alors la sortie du dispositif de sélection 228 fournit sur sa sortie le nombre "zéro" codé sur k + 1 bits. Lorsque le premier signal de sélection

SELA est à un niveau logique « un » et que le deuxième signal de sélection SELY est à un niveau logique « zéro », alors la sortie du dispositif de sélection 228 fournit sur sa sortie le contenu de la première bascule 225. Lorsque le premier signal de sélection SELA est à un niveau logique « zéro » et que le deuxième signal de sélection SELY est à un niveau logique « un », alors la sortie du dispositif de sélection 228 fournit sur sa sortie le contenu de la deuxième bascule 226. Lorsque les premier et deuxième signaux SELA et SELY de sélection sont tous deux à un niveau logique « un », alors la sortie du dispositif de sélection 228 fournit sur sa sortie la somme des contenus des première et deuxième bascules 225 et 226.

- Un cinquième multiplexeur 229, disposant de deux entrées et d'une sortie, a sa sortie connectée à la première entrée de sélection du dispositif de sélection 228. l'une des entrées du cinquième multiplexeur 229 est connectée à la sortie du premier circuit de retard 211. L'autre des entrées du cinquième multiplexeur 229 reçoit un « zéro » logique.

- Un sixième multiplexeur 230, disposant de première à troisième entrées et d'une sortie, a sa sortie connectée à la deuxième entrée de sélection du dispositif de sélection 228. La première entrée du sixième multiplexeur 230 reçoit un « zéro » logique. La deuxième entrée du sixième multiplexeur 230 est connectée à la sortie du troisième circuit de retard 213.

- Un circuit accumulateur 231 effectue une double multiplication par addition successive des mots sortant du dispositif de sélection 228. Le circuit accumulateur 231 comporte une entrée parallèle connectée à la sortie du dispositif de sélection 228, une entrée série connectée à la sortie du quatrième circuit de retard 214, une sortie de résultat et trois sorties de valeurs internes notées I_0 à I_2. Lors de chaque cycle de l'horloge

de séquencement du coprocesseur 200, le circuit accumulateur additionne un bit présent à l'entrée série avec un mot présent à l'entrée parallèle et avec un résultat interne. Le nouveau résultat est ensuite décalé pour devenir un nouveau résultat interne.

- Un septième multiplexeur 233 dispose de deux entrées et d'une sortie. L'une des entrées du septième multiplexeur 233 est connectée à la sortie de résultat du circuit accumulateur 231. La sortie du septième multiplexeur 233 est connectée aux deuxièmes entrées des dispositifs de mémorisation 201 à 204.

- Une porte ET 234 dispose de première et deuxième entrées et d'une sortie. La première entrée de la porte ET 234 est connectée à la sortie du premier circuit de soustraction 205. La deuxième entrée de la porte ET 234 est connectée à un conducteur de la sortie parallèle de la première bascule 225 qui correspond au bit de poids le plus faible du mot contenu dans la première bascule 225.

- Une porte OU Exclusif 235 dispose de première à cinquième entrées et d'une sortie. Une première entrée de la porte OU Exclusif 235 est connectée à la sortie de la porte ET 234. une deuxième entrée de la porte OU Exclusif 235 est connectée à la sortie du deuxième circuit de soustraction 206. les troisième à cinquième entrées de la porte OU Exclusif 235 sont connectées respectivement aux trois sorties de valeurs internes du circuit accumulateur 231.

- Un huitième multiplexeur 236 dispose de deux entrées et d'une sortie. L'une des entrées du huitième multiplexeur 236 est connectée à la sortie série du premier registre 221. L'autre des entrées du huitième multiplexeur 236 est connectée à la sortie série du premier circuit de retard 211. La sortie du huitième multiplexeur 236 est connectée à l'autre entrée du septième multiplexeur 233.

- Un circuit de comparaison 232 disposant de deux

entrées compare bit à bit le résultat sortant du circuit accumulateur 231 avec la donnée qui sort en série du huitième multiplexeur 236. Le résultat de la comparaison est ensuite transmis à un circuit de gestion (non représenté) du coprocesseur 200.

La figure 2 représente un cheminement de données entre différents éléments fonctionnels. Le cheminement représenté à l'aide des conducteurs de liaisons et des différents multiplexeurs peut présenter de nombreuses variantes, l'important étant d'assurer des échanges de données entre les différents éléments de calcul et de mémorisation.

Certains éléments de la figure 2 ne correspondent pas exactement à des éléments standards couramment utilisés par l'homme du métier. Les figures 3 à 7 précisent la structure de ces différents éléments.

La figure 3 correspond à l'un des dispositifs de mémorisation 201 à 204. Le dispositif de mémorisation 201 comporte deux multiplexeurs 301 et 302 et des premier à m-ième registres à décalage 303 notés également R1 à Rm.

Le multiplexeur 301 comporte des première à quatrième entrées et une sortie. Les première et deuxième entrées du multiplexeur 301 constituent les première et deuxième entrées du dispositif de mémorisation 201. La troisième entrée du multiplexeur 301 reçoit un "zéro" logique.

Les premier à m-ième registres 303 sont des registres de k bits, à décalage, qui disposent d'une entrée série et d'une sortie série. Les entrées des premier à m-ième registres 303 sont connectées ensembles à la sortie du multiplexeur 301.

Le multiplexeur 302 comporte des première à m-ième entrées et une sortie. Les premières à m-ième entrées du multiplexeur 302 sont respectivement connectées aux sorties des premier à m-ième registres 303. La sortie du multiplexeur 302 est connectée à la quatrième entrée du

multiplexeur 301.

Des signaux de commande (non représentés) servent à sélectionner les entrées des multiplexeurs 301 et 302 et à valider le décalage de manière indépendante dans chacun des registres 303.

Lorsque l'on désire mémoriser une donnée de m * k bits dans le dispositif de mémorisation 201, ladite donnée est rangée par mot de k bits dans chacun des registres 303. Pour mémoriser la donnée, il suffit d'effectuer k décalages du premier registre 303, puis k décalages du deuxième registre 303 et ainsi de suite jusqu'au m-ième registre 303, le multiplexeur 301 sélectionnant la source de la donnée.

Pour fournir une donnée codée sur m * k bits, il suffit de décaler les uns après les autres les registres 303 dans l'ordre de mémorisation de la donnée.

Le bouclage de la sortie du multiplexeur 302 sur la quatrième entrée du multiplexeur 301 permet de faire entrer dans l'un des registres 303 le mot de k bits qui est sorti simultanément. Ce bouclage assure la mémorisation des données que l'on sort pour des usages multiples.

Comme on peut le remarquer il est possible d'utiliser de manière indépendante n'importe quel mot de k bits d'une donnée comportant plusieurs mots de k bits. Il est également possible de faire entrer un mot de k bits dans l'un des registres 303 pendant que l'on sort un mot de k bits d'un autre des registres 303.

La figure 4 représente le premier (ou le deuxième) circuit de soustraction 205 (ou 206). Le circuit de soustraction 205 comporte deux inverseurs 401 et 402, un additionneur élémentaire et deux bascules 404 et 405 de mémorisation de type D, connectés selon une technique connue, comme indiqué sur la figure 4.

Ce circuit de soustraction 205 produit un retard systématique d'un cycle d'horloge sur les données le

traversant. Le deuxième circuit de retard 212 sert à compenser les retards produits sur les données qui sortent du troisième dispositif de mémorisation 203. De même, on pourrait également compenser les retards sur la sortie du premier dispositif de mémorisation 201. Cependant, les données sortantes du premier dispositif de mémorisation 201 n'ont pas besoin d'être synchroniser avec les autres données.

L'utilisation de circuit de soustraction 205 tel que représenté sur la figure 4 permet également de s'affranchir des premier, troisième et quatrième circuits de retard 211, 213 et 214. En effet, la bascule 404 produit un retard identique. Il suffit d'extraire le signal à l'entrée de la bascule 404 et de l'inverser pour obtenir le prochain bit sortant. Un inconvénient est de ne pas avoir un signal stable dès le front actif du signal d'horloge. Pour les systèmes fonctionnant avec une fréquence d'horloge peu élevée, cela permet d'économiser trois bascules D.

Le circuit de la figure 5 représente le circuit de comparaison 232 de manière détaillée. Le circuit de comparaison 232 correspond à un circuit de soustraction sur lequel on extrait la retenue mémorisée et la donnée qui arrive sur la première entrée du circuit de soustraction, le circuit de soustraction étant bien évidemment simplifié. La retenue mémorisée est inversée puis rentre dans un OU logique avec la donnée présente sur la première entrée. Le résultat sortant du OU logique lorsque la totalité des données est rentrée dans le circuit de comparaison 232 permet de savoir laquelle des deux données est supérieure à l'autre. Le résultat est mémorisé dans une bascule D 501.

La bascule D 501 dispose d'une entrée de donnée, d'une entrée d'horloge, d'une entrée de forçage à « un », d'une entrée de forçage à « zéro », et d'une sortie. L'entrée de donnée reçoit la donnée sortant du OU

logique, l'entrée d'horloge reçoit un signal de chargement LD dont le front montant correspond à l'instant où l'on désire obtenir le résultat de la comparaison. Les entrées de forçage à « un » et à « zéro », reçoivent des signaux de prépositionnement ST et RST pour initialiser le circuit de comparaison 232. La sortie de la bascule 501 est connectée à un dispositif de séquencement (non représenté) du coprocesseur 200.

La figure 6 représente un élément du dispositif de sélection 228. Le dispositif de sélection comporte k + 1 éléments de ce type. Cet élément est constitué de trois porte ET 601 à 603 à trois entrées, deux portes ET 601 et 603 ayant une entrée inverseuse, et d'une porte OU 604 à trois entrées. Le rôle de cet élément est le même que celui d'un multiplexeur à quatre entrées dont la quatrième entrée reçoit un "zéro" logique. Dans le dispositif de sélection 228, l'élément correspondant au bit de poids le plus fort ne comporte que la porte ET centrale 602 car les première et deuxième bascules 224 et 225 ne disposent que de k bits.

La figure 7 représente un ensemble constitué par le circuit accumulateur 231 et le dispositif de sélection 228. L'ensemble ainsi constitué réalise deux multiplications avec addition des deux produits et addition d'une autre donnée en série. Si on appelle LATCHA la donnée présente dans la première bascule 225, LATCHY la donnée présente dans la deuxième bascule 226, SELA la donnée arrivant en série sur la première entrée de sélection du dispositif de sélection 228, SELY la donnée arrivant en série sur la deuxième entrée de sélection du dispositif de sélection, ES la donnée arrivant en série sur l'entrée série de l'accumulateur 231, et RES le résultat sortant de l'accumulateur 231, alors on effectue l'opération suivante :

RES = (SELY * LATCHY) + (SELA * LATCHA) + ES

La structure du circuit accumulateur 231 correspond

à une structure standard d'accumulateur. Ledit circuit 231 comporte :

- des première à k-ième bascules d'accumulation 701 à 704, par exemple de type D, disposant chacune d'une entrée de donnée et d'une sortie, l'entrée de donnée de la première bascule 701 étant connectée au conducteur de poids le plus fort (c'est à dire de poids k) de la sortie parallèle du dispositif de sélection 228 ;
- des première à (k+1)-ième bascules de retenue 705 à 709, par exemple de type D, disposant chacune d'une entrée de donnée et d'une sortie ;
- une bascule de résultat 710, par exemple de type D, disposant d'une entrée de donnée et d'une sortie, la sortie de cette bascule de résultat correspondant à la sortie de l'accumulateur 231 ;
- des premier à (k+1)-ième additionneurs 711 à 715 standards (ou additionneur complet) disposant chacun de première à troisième entrées, d'une sortie de résultat, et d'une sortie de retenue, les premières entrées des premier à k-ième additionneurs 711 à 714 étant connectées au dispositif de sélection 228 pour recevoir respectivement les bits de poids k-1 à 0, les deuxièmes entrées des premier à k-ième additionneurs 711 à 714 étant connectées respectivement aux sorties des première à k-ième bascules d'accumulation 701 à 704, la première entrée du (k+1)-ième additionneur 715 étant connectée à la sortie de résultat du k-ième additionneur 714, la deuxième entrée du (k+1)-ième additionneur 715 correspondant à l'entrée série de l'accumulateur 231 qui reçoit la donnée ES, les troisièmes entrées des premier à (k+1)-ième additionneurs 711 à 715 étant respectivement connectées aux sorties des première à (k+1)-ième bascules de retenue 705 à 709, les sorties de résultat des premier à (k-1)-ième additionneurs 711 à 713 étant respectivement connectées aux entrées de données des deuxième à k-ième bascules d'accumulation 702 à 704, la sortie de résultat

du (k+1)-ième additionneur 715 étant connectée à l'entrée de la bascule de résultat 710, les sorties de retenue des premier à (k+1)-ième additionneurs 711 à 715 étant respectivement connectées aux entrées de données des première à (k+1)-ième bascules de retenue 705 à 709.

Les sorties internes I_0 à I_2 correspondent respectivement aux sorties de retenue des k+1-ième et k-ième additionneurs 715 et 714 et à la sortie de résultat du (k-1)-ième additionneur 713.

Dans la pratique, les bascules de retenue, d'accumulation et de résultat 701 à 710 comportent également des entrées d'horloge et de forçage à zéro. Toutes les entrées d'horloge desdites bascules 701 à 710 sont connectées ensembles et reçoivent un même signal d'horloge. De même, toutes les entrées de forçage à zéro sont connectées ensemble pour être remise à zéro simultanément avant chaque calcul. Ces entrées ne sont pas représentées pour ne pas surcharger inutilement les dessins.

Le fonctionnement du dispositif décrit sur cette figure 7 est relativement simple. Lors de chaque cycle du signal d'horloge qui synchronise le coprocesseur, on additionne successivement soit LATCHA, soit LATCHY, soit LACHA + LATCHY, soit zéro avec le contenu des bascules de retenue 705 à 709 et avec le bit arrivant de la donnée ES au contenu des bascules d'accumulation 701 à 704, le mot contenu dans les bascules d'accumulation 701 à 704 étant décalé successivement, de sorte que le bit contenu dans la bascule de résultat 710 corresponde au bit qui sort de l'accumulateur 231.

Avant de commencer un calcul, on effectue une remise à zéro de toutes les bascules d'accumulation, de retenue et de résultat 701 à 710. Puis, la double multiplication s'effectue ensuite par décalage simultané des données SELA, SELY et ES, à chaque cycle du signal d'horloge. Les bits de SELA et de SELY déterminent

quelle(s) donnée(s) parmi LATCHA et LATCHY doivent être accumulées (voir le fonctionnement du dispositif de sélection 228). Lorsque la totalité des bits des données SELA et SELY a été décalée (soit après m * k cycles d'horloge), on fournit des "0" (pendant k+1 cycles d'horloge) à la place des données SELA, SELY et ES afin de sortir la fin du résultat encore contenu dans les bascules d'accumulation 701 à 704.

Si lesdites données sont codées sur des nombres de bits différents, il convient de compléter chaque donnée à l'aide de « 0 ».

A présent que la description structurelle et fonctionnelle des éléments composant le coprocesseur a été faite, il convient d'expliquer à présent le fonctionnement global du coprocesseur. Les explications qui vont suivrent permettront à l'homme du métier de synchroniser de manière globale le coprocesseur afin d'obtenir les opérations désirées. Par la suite, on utilise les données A, B et N qui sont des entiers non nuls codés sur respectivement a * k, b * k et n * k bits, avec a, b et n des entiers non nuls inférieurs à m. Dans un premier temps, on considère N impair.

Opération élémentaire $P_{field}(A, B)_N = A*B*I \bmod N$:

A) Initialisation du coprocesseur :

- On charge les données A, B, N respectivement dans les premier à troisième dispositifs de mémorisation 201 à 203 ;
- On charge des zéros dans le quatrième dispositif de mémorisation 204, la donnée étant appelée S(-1) ;
- On initialise le dispositif de comparaison 232 pour que la dernière comparaison indique que N est supérieur à S(-1).

B) Répétition a fois de la boucle de calcul suivante, avec i un indice variant de 0 à a-1 :

B-1) On charge simultanément le i-ième mot A_i de poids faible de A dans le premier registre 221 et

le mot N_0 de poids le plus faible de N dans le deuxième registre 222.

B-2) Puis, on charge simultanément les mots A_i et N_0 respectivement dans les première et deuxième bascules 225 et 226.

B-3) On initialise à zéro les circuits de soustraction 205 et 206, les circuits de retard 211 à 214, le premier registre 221 et toutes les bascules 701 à 710 de l'accumulateur 231.

B-4) On décale simultanément de deux unités les mots B, N et S(i-1) contenus dans les deuxième à quatrième dispositifs de mémorisation 202 à 204, des zéros étant fournis sur les première et deuxième entrées du dispositif de sélection 228.

B-5) On effectue k décalages successifs sur les deuxième à quatrième dispositifs de mémorisation 202 à 204, sur les premier et deuxième registres 221 et 222. La sortie de la porte OU Exclusif 235 fournit successivement les k bits d'une donnée Y_0, avec $Y_0 = ((S(i-1) + A_i * B) * J_0) \bmod 2^k$, J0 étant défini par l'équation $((N*J_0)+1) \bmod 2^k = 0$. La sortie de la porte OU Exclusif est reliée d'une part à l'entrée du deuxième registre 222 et d'autre part à la deuxième entrée de sélection du dispositif de sélection 228. La donnée B est fournie à la première entrée de sélection du dispositif de sélection. L'entrée du premier registre 221 reçoit bit à bit le mot N_0 de poids faible de N. L'entrée série de l'accumulateur reçoit S(i-1) si la dernière comparaison indique que $S(i-1) < N$, ou reçoit $S(i-1) - N$ si la dernière comparaison indique que $S(i-1) \geq N$ (la soustraction s'effectuant dans le deuxième circuit de soustraction 206). La sortie de l'accumulateur 231 fournit k bits égaux à zéro qui ne sont pas mémorisés.

B-6) On transfert le contenu du deuxième registre 222 égal à Y_0 dans la deuxième bascule 226.

B-7) On effectue (n-1) * k décalages successifs sur les deuxième à quatrième dispositifs de mémorisation 202 à 204 et sur le premier registre 221. La donnée B est fournie à la première entrée de sélection du dispositif de sélection. Les n-1 mots N_1 à N_{n-1} de poids fort de N sont fournis bit à bit d'une part à l'entrée du premier registre 221 et d'autre part à la deuxième entrée de sélection du dispositif de sélection 228. L'entrée série du circuit accumulateur 231 reçoit S(i-1) si la dernière comparaison indique que S(i-1) < N, ou reçoit S(i-1) - N si la dernière comparaison indique que S(i-1) ≥ N (la soustraction s'effectuant dans le deuxième circuit de soustraction 206). La sortie du circuit accumulateur 231 fournit les (n-1) * k bits de poids faible de S(i) qui sont mémorisés dans le quatrième dispositif de mémorisation 204. Les (n-1) * k bits de poids faible de S(i) sont comparés avec les (n-1) * k bits de poids faible de N dans le circuit de comparaison 232.

B-8) On effectue k+1 décalages successifs sur le quatrième dispositif de mémorisation 204 et sur le premier registre 221. Les première et deuxième entrées de sélection du dispositif de sélection 228 reçoivent des zéros pour pouvoir fournir les k bits de poids fort de S(i) et finir la comparaison de S(i) avec N. Le résultat de la comparaison est mémorisé pour la prochaine itération.

C) A l'issue de la dernière itération, le résultat S(a-1) mémorisé dans le quatrième dispositif de mémorisation subit une nouvelle soustraction de N si S(a-1) ≥ N. La soustraction s'effectue par décalage simultané de

S(a-1) et N dans le deuxième circuit de soustraction 206. Pour récupérer le résultat de la soustraction, on fournit des zéros aux entrées de sélection du dispositif de sélection 228 afin de rendre transparent le circuit accumulateur 231.

L'homme du métier peut remarquer que la donnée de calcul J_0 n'est plus calculée. En effet, les connexions réalisées sur les entrées de la porte OU Exclusif permettent de calculer directement Y_0 avec un décalage d'un cycle d'horloge par rapport au calcul de S(i).

De même, l'homme du métier peut remarquer que l'on commence le calcul avec N_0 dans la deuxième bascule 222 puis que l'on remplace N_0 par Y_0. Le résultat est exactement le même que si l'on avait Y_0 dans la deuxième bascule 222 en fournissant N en série sur la deuxième entrée de sélection depuis le début du calcul.

L'homme du métier peut remarquer qu'avantageusement le premier registre 221 est utilisé d'une part pour transférer un mot dans la première bascule 225, et d'autre part pour retarder N de k cycles d'horloge.

Multiplication modulaire :

Pour effectuer une multiplication modulaire, il suffit d'effectuer deux opérations élémentaires P_{field} en introduisant un paramètre H de correction d'erreur. On effectue ainsi soit $P_{field}(H, P_{field}(A, B)_N)_N$, soit $P_{field}(A, P_{field}(H, B)_N)_N$, avec $H = 2^{(a+n)*k} \bmod N$.

Calcul de $A^C \bmod N$

On pose C un entier codé sur c bits et dont le bit de poids 2^{c-1} est égal à 1. On considère que A et N sont codés sur un même nombre de bit égal à n*k bits. Si A est de taille inférieure à N, alors on complète A avec des zéros en bits de poids fort.

a) on calcule $H = 2^{2*n*k} \bmod N$.

b) on calcule $R(1) = P_{field}(H, A)$, et on mémorise R(1) dans les premier et deuxième dispositifs de mémorisation 201 et 202, le contenu du premier

dispositif 201 étant appelé A, et le contenu de deuxième dispositif 202 étant appelé B.

c) on effectue une boucle indexée par un indice i variant de 2 à c :

c-1) On effectue une opération $P_{field}(B, B)_N$, en chargeant les mots de B à la place des mots de A lors de l'étape B-1. Le résultat est stocké dans le deuxième dispositif de mémorisation 202.

c-2) Si le bit de poids 2^{c-i} de C est égal à 1 alors on effectue également une opération $P_{field}(A, B)_N$, et on stocke le résultat dans le deuxième dispositif de mémorisation 202.

d) On charge « 1 » codé sur n*k bits dans le premier dispositif de mémorisation 201.

e) On effectue une opération $P_{field}(1, B)_N$ pour obtenir le résultat final.

Calcul de $H = 2^{(n+p)*k} \bmod N$, p étant un entier

Pour effectuer le calcul de H, on neutralise une partie des éléments du coprocesseur 200. Le cinquième multiplexeur 229 est positionné pour fournir des « zéro » sur sa sortie. On charge une donnée égale à « 1 » codé sur k bits dans la deuxième bascule 226. Le sixième multiplexeur 230 est positionné pour relier la sortie du troisième circuit de retard 213 à la deuxième entrée de sélection du dispositif de sélection 228. Le huitième multiplexeur 236 est positionné pour relier l'entrée du comparateur 232 à la sortie du premier circuit de retard 211. L'ensemble résultant de ces différentes neutralisations transforme le coprocesseur 200 en circuit de calcul de H par soustractions successives. Un tel circuit est décrit dans la demande européenne n°0 601 907.

REVENDICATIONS

1. Circuit intégré comprenant un coprocesseur (200) d'arithmétique modulaire comportant :

- des moyens de mémorisation (201 à 204) pour mémoriser et fournir en série des premier et deuxième opérandes A et B, un modulo N et un résultat S, avec A un entier codé sur a * k bits, a étant un entier non nul au plus égal à m, et avec B, N et S qui sont des entiers codés sur au plus m * k bits, m et k étant des entiers supérieurs à 1 ;

- des moyens de calcul pour effectuer des opérations modulaires selon la méthode de Montgomery,

caractérisé en ce que les moyens de calcul comportent :

- un circuit (234, 235) pour calculer une donnée intermédiaire Y_0 ;

- une première bascule (225) de k bits pour mémoriser un mot A_i de k bits de A ;

- une deuxième bascule (226) de k bits pour mémoriser soit le mot de poids le plus faible de N soit Y_0 ;

- un circuit parallèle d'addition (227) connecté pour additionner les mots contenus dans les première et deuxième bascules (225, 226) ;

- un dispositif de sélection (228) couplé aux sorties des première et deuxième bascules (225, 226) et du circuit parallèle d'addition (227) afin de fournir sur une sortie parallèle soit le mot contenu dans la première bascule (225), soit le mot contenu dans la deuxième bascule (226), soit la somme des mots contenus dans les première et deuxième bascules (225, 226), soit "zéro", en fonction d'une part d'un bit de B, et d'autre part soit d'un bit de Y_0 soit d'un bit de N ;

- un circuit accumulateur (231) qui additionne, décale d'un bit et mémorise les mots fournis

successivement par le dispositif de sélection (228) avec un bit d'un résultat actualisé S, les bits sortant du circuit accumulateur (231) devenant un nouveau résultat actualisé.

2. Circuit selon la revendication 1, caractérisé en ce que les moyens de calcul comportent un premier registre (221) à décalage de k bits pour recevoir d'une part un mot de k bits de A et transmettre ledit mot en parallèle à la première bascule (225) et d'autre part N afin de retarder N de k cycles d'un signal d'horloge.

3. Circuit selon la revendication 1, caractérisé en ce que le circuit pour calculer la donnée Y_0 est constitué d'une porte de type OU Exclusif (235) à cinq entrées qui reçoit une première donnée provenant d'unè porte de type ET logique (234) entre le bit de poids faible du mot de A présent dans la première bascule (225) et le prochain bit de B à fournir au dispositif de sélection (228), une deuxième donnée correspondant au prochain bit de S à fournir au circuit accumulateur (231), et à des troisième à cinquième données qui correspondent à des valeurs internes du circuit accumulateur (231).

4. Procédé pour effectuer une opération modulaire selon la méthode de Montgomery par décalage en série de premier et deuxième opérandes A et B, d'un modulo N et d'un résultat actualisé à travers des moyens de calcul, avec A un entier codé sur a * k bits, a étant un entier non nul au plus égal à m, et avec B, N et S qui sont des entiers codés sur au plus m * k bits, m et k étant des entiers supérieurs à 1 caractérisé en ce qu'il comporte la répétition des étapes suivantes, i étant un indice variant de 0 à m-1 :

- mémorisation d'un mot A_i de k bits correspondant à un mot de poids i de A dans une première bascule (226) de k bits ;

- calcul d'une donnée intermédiaire Y_0 telle que $Y_0 = ((S(i-1) + (Ai * B)) * J_0) \mod 2^k$, avec S(i-1) qui

correspond au (i-1)-ième résultat actualisé, S(-1) étant égal à 0, et J_0 étant un mot de k bits résolvant l'équation $((J_0 * N) + 1) \bmod 2^k = 0$;

- mémorisation du mot de k bits de poids faible de N puis de Y_0 dans une deuxième bascule (226) de k bits ;

- addition dans un circuit parallèle d'addition (227) des mots contenus dans les première et deuxième bascules (225, 226);

- sélection et fourniture soit du mot contenu dans la première bascule (225), soit du mot contenu dans la deuxième bascule (226), soit de la somme des mots contenus dans les première et deuxième bascules (225, 226), soit "zéro", en fonction d'une part d'un bit de B, et d'autre part soit d'un bit de Y_0 soit d'un bit de N;

- Additions successives dans un circuit accumulateur (231) des mots fournis par le dispositif de sélection (228) pour chaque paire de bits de B et de N, le résultat de chaque addition étant additionné à un bit du précédent résultat actualisé S(i-1) puis décalé d'un bit et mémorisé entre chaque addition, le bit sortant de l'accumulateur (231) lors du décalage correspondant à un nouveau résultat actualisé S(i).

5. Procédé selon la revendication 4, caractérisé en ce que l'on effectue une comparaison du résultat sortant de l'accumulateur (231) avec N retardé de k cycles d'un signal d'horloge, et en ce que l'on utilise un même premier registre (221) à décalage de k bits pour retarder N et pour pouvoir charger les mots A_i dans la première bascule (225).

6. Procédé selon l'une des revendications 4 ou 5, caractérisé en ce que la mémorisation d'un mot A_i dans la première bascule (225) s'effectue par k décalages du mot A_i dans le premier registre (221) puis chargement parallèle dans la première bascule (225) après que le mot A_i ait été chargé en entier dans le premier registre (221).

7. Procédé selon l'une des revendications 4 à 6, caractérisé en ce que le calcul de chaque bit de la donnée intermédiaire Y_0 s'effectue un cycle d'horloge avant que l'on ait besoin dudit chaque bit.

8. Procédé selon la revendication 4, dans lequel on effectue les étapes suivantes

A) Initialisation du coprocesseur :

- chargement des données A, B, N respectivement dans des premier à troisième dispositifs de mémorisation (201 à 203) ;
- chargement de zéros dans un quatrième dispositif de mémorisation (204), la donnée étant appelée S(-1) ;
- initialisation d'un dispositif de comparaison (232) pour qu'une dernière comparaison indique que N est supérieur à S(-1) ;

B) répétition a fois de la boucle suivante, avec i un indice variant de 0 à a-1 :

B-1) chargement simultané du i-ième mot A_i de poids faible de A dans un premier registre (221) de k bits et du mot N_0 de poids le plus faible de N dans un deuxième registre (222) de k bits ;

B-2) puis, chargement simultané des mots A_i et N_0 respectivement dans les première et deuxième bascules (225, 226) ;

B-3) initialisation des circuits de soustraction (205, 206), des circuits de retard (211 à 214), du premier registre (221) et du circuit accumulateur (231) ;

B-4) décalage simultané des mots B, N et S(i-1) contenus dans les deuxième à quatrième dispositifs de mémorisation (202 à 204), des zéros étant fournis au dispositif de sélection (228) ;

B-5) réalisation de k décalages successifs sur les deuxième à quatrième dispositifs de mémorisation (202 à 204), sur les premier et deuxième

registres (221, 222), des moyens de calcul fournissant successivement les k bits de la donnée Y_0 d'une part au deuxième registre (222) et d'autre part au dispositif de sélection (228), la donnée B étant fournie également au dispositif de sélection (228), le premier registre (221) recevant bit à bit le mot N_0 de k bits de poids faible de N, l'accumulateur (231) recevant en série S(i-1) si la dernière comparaison indique que $S(i-1) < N$, ou recevant en série $S(i-1) - N$ si la dernière comparaison indique que $S(i-1) \geq N$;

B-6) transfert du contenu du deuxième registre (222) égal à Y_0 dans la deuxième bascule (226) ;

B-7) réalisation de (n-1) * k décalages successifs sur les deuxième à quatrième dispositifs de mémorisation (202 à 204) et sur le premier registre (221), la donnée B étant fournie au dispositif de sélection (228), les n-1 mots N_1 à N_{n-1} de k bits de poids fort de N étant fournis bit à bit d'une part au premier registre (221) et d'autre au dispositif de sélection (228), l'accumulateur (231) recevant en série S(i-1) si la dernière comparaison indique que $S(i-1) < N$ ou recevant en série $S(i-1) - N$ si la dernière comparaison indique que $S(i-1) \geq N$, l'accumulateur (231) fournissant les (n-1) * k bits de poids faible de S(i) qui sont mémorisés dans le quatrième dispositif de mémorisation (204), les (n-1) * k bits de poids faible de S(i) étant comparés avec les (n-1) * k bits de poids faible de N dans le circuit de comparaison (232) ;

B-8) réalisation de k+1 décalages successifs sur le quatrième dispositif de mémorisation (204) et sur le premier registre (221), pour pouvoir mémoriser

les k bits de poids fort de S(i) et finir la comparaison de S(i) avec N, le résultat de la comparaison étant mémorisé pour la prochaine itération.

5

2791157

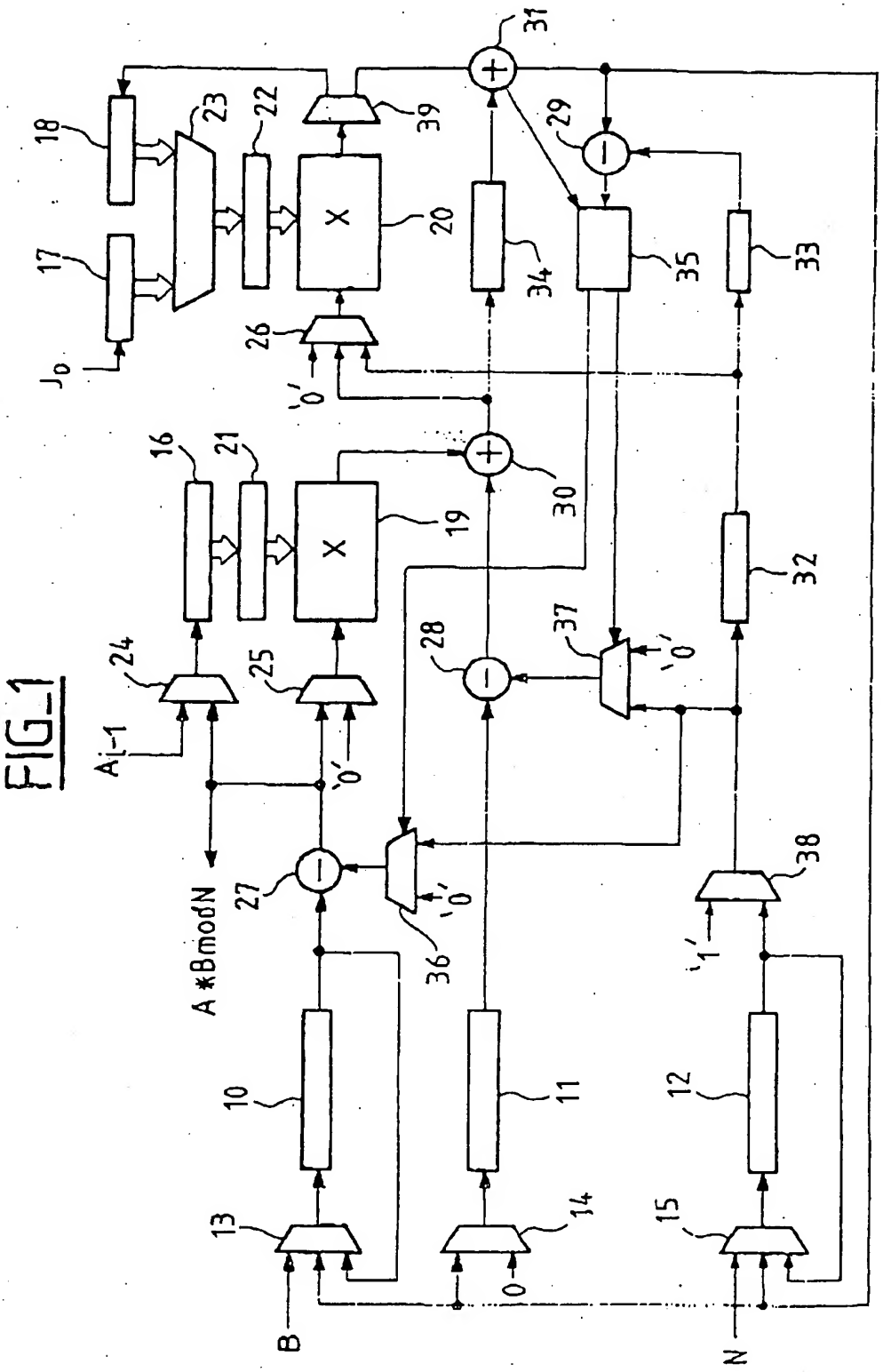


FIG_1

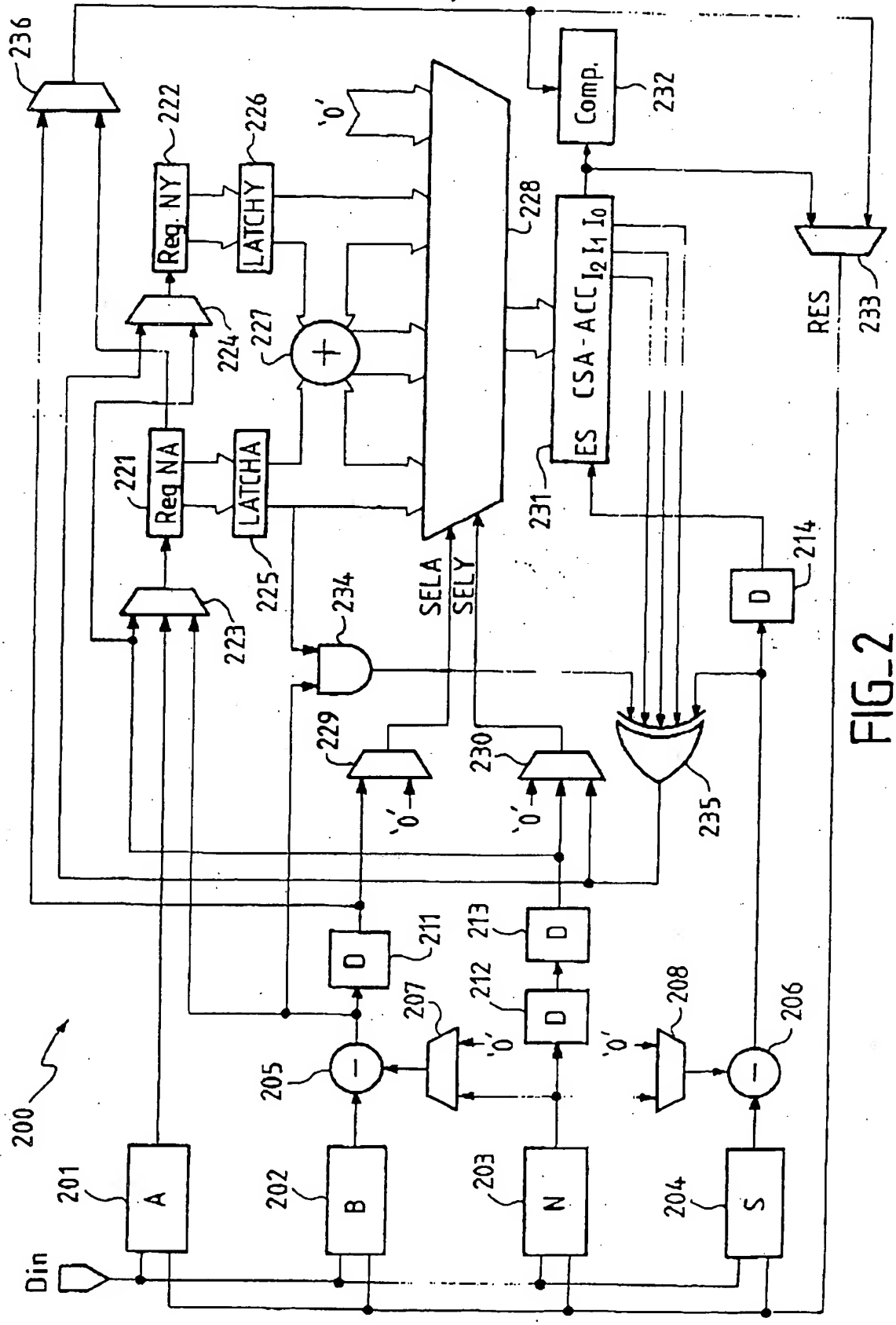

236
222
226
'0'
Comp.
232
Reg. NY
LATCHY
228
224
227
CSA - ACC
I2 I1 I0
RES
233
221
Reg NA
LATCHA
231
ES
214
D
225
234
SELA
SELY
223
229
230
'0'
'0'
235
D
211
213
D
D
212
207
208
206
'0'
'0'
205
200
201
202
203
204
A
B
N
S
Din

FIG_2

2791157

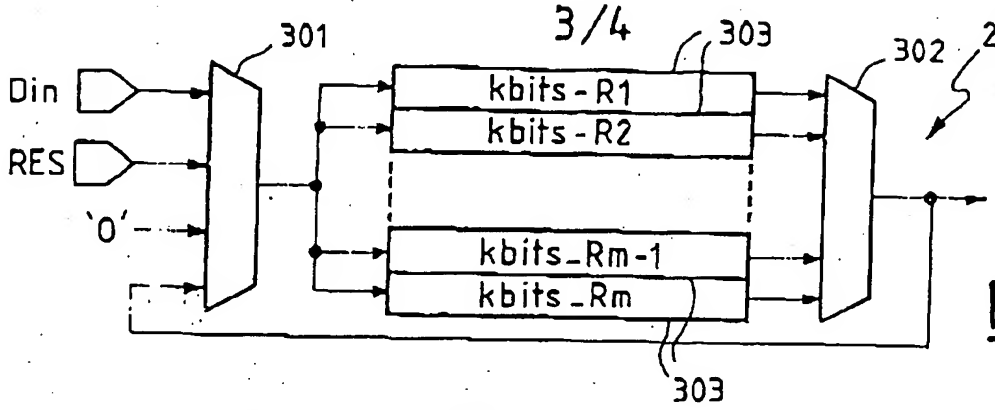


FIG_3

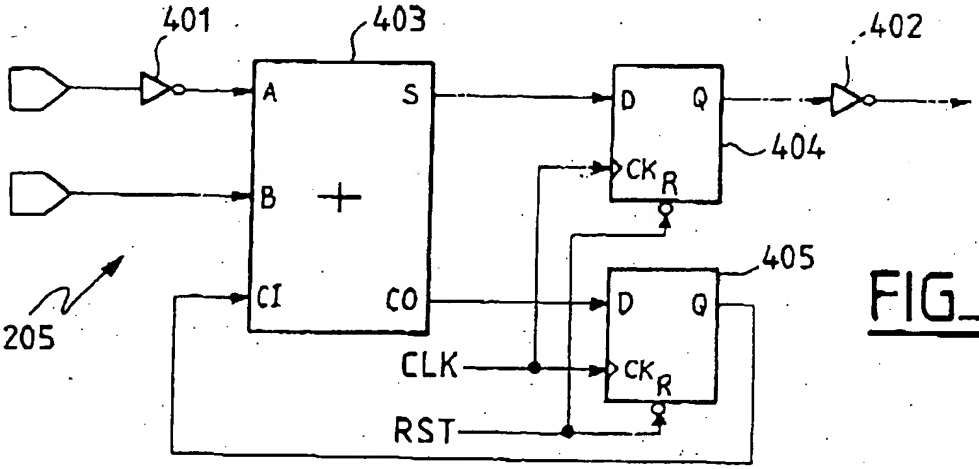


FIG_4

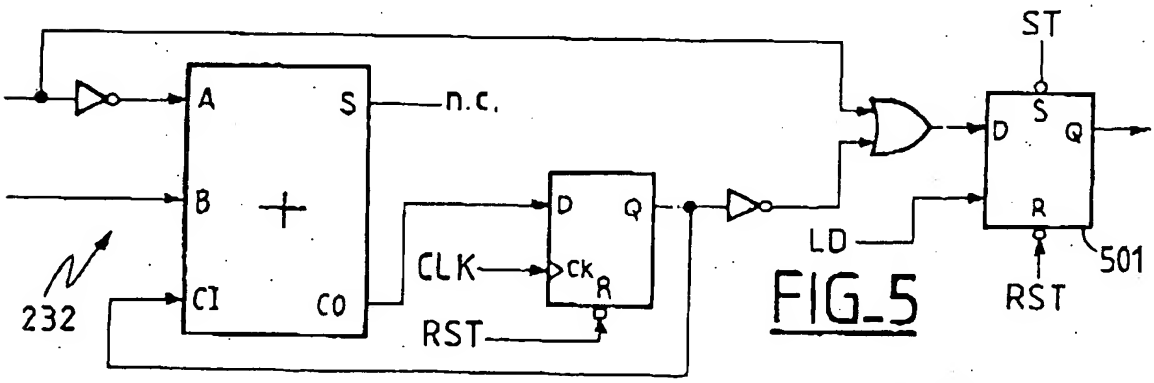


FIG_5

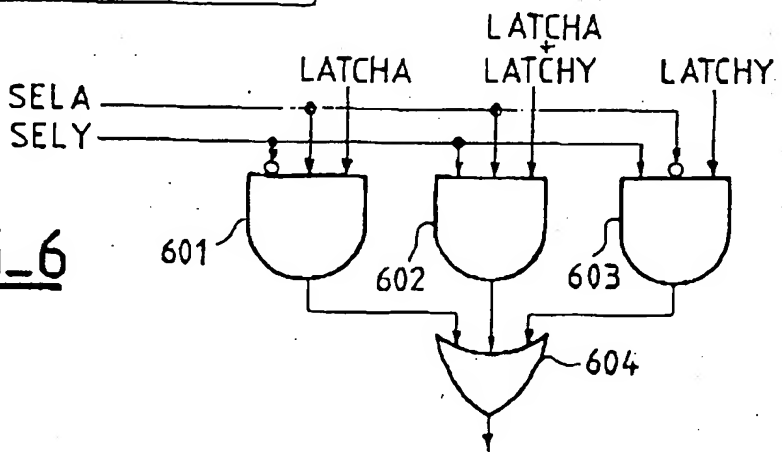
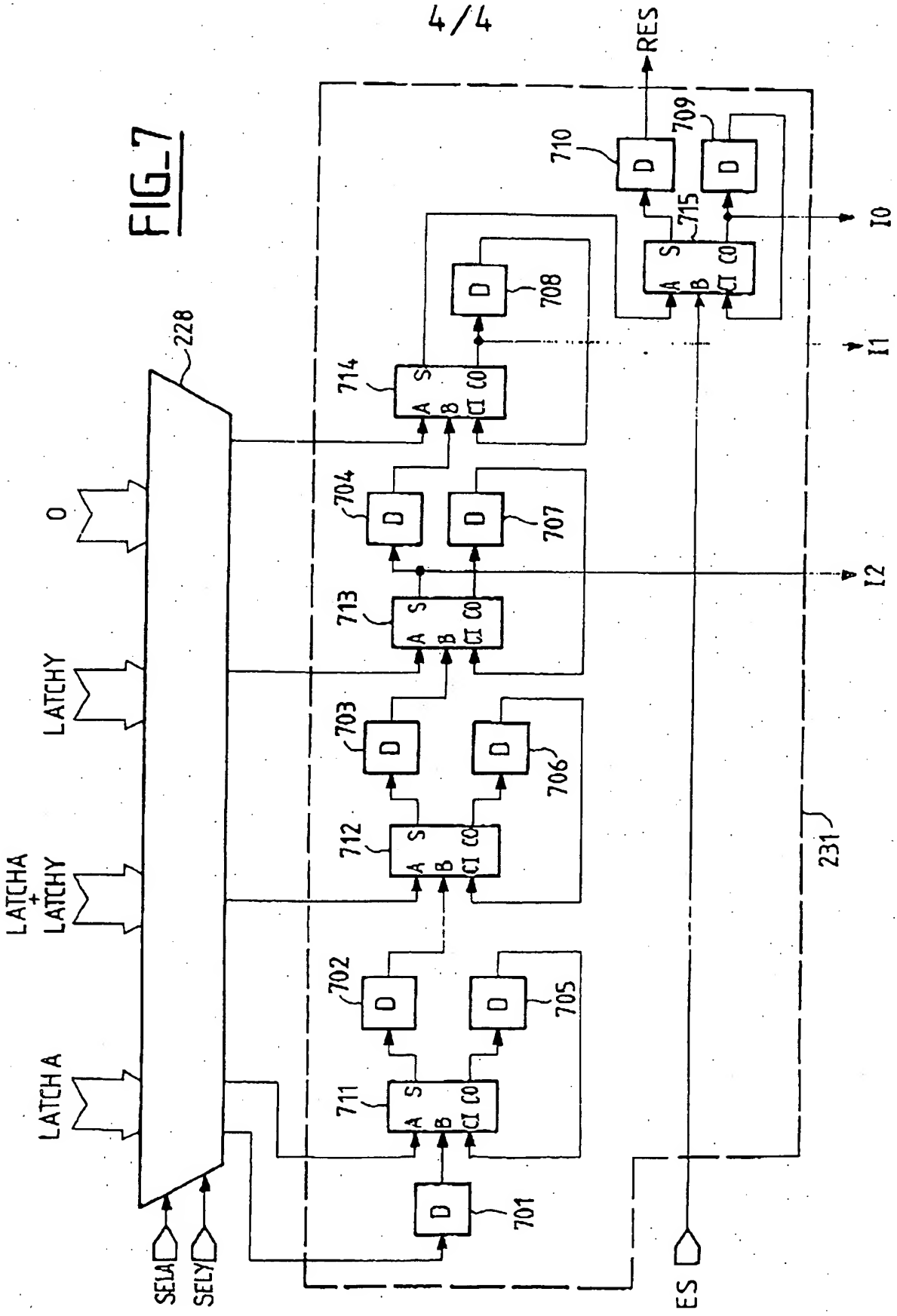


FIG_6

FIG_7


RES
709
710
715
I0
I1
I2
708
714
228
0
704
707
713
LATCHY
703
706
712
LATCHA
+
LATCHY
231
702
705
711
LATCH A
701
SELA
SELY
ES

RÉPUBLIQUE FRANÇAISE

2791157

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 578463
FR 9903410

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
X	WO 98 50851 A (GRESSEL CARMI DAVID ;DROR ITAI (IL); HADAD ISAAC (IL); ARAZI BENJA) 12 novembre 1998 (1998-11-12) * page 13, ligne 16 - ligne 27; figure 1B * -----	1-8

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.7)

G06F

Date d'achèvement de la recherche: 26 janvier 2000

Examinateur: Verhoof, P

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)

1